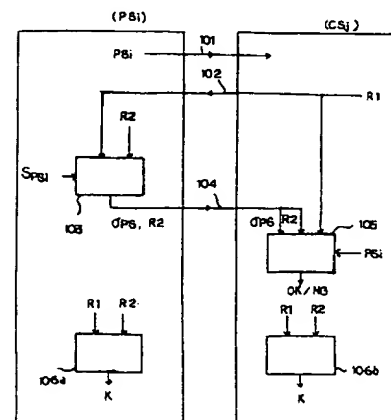


**(54) COMMUNICATION METHOD FOR RADIO COMMUNICATION SYSTEM**

(11) 5-347617 (A) (43) 27.12.1993 (19) JP  
 (21) Appl. No. 4-154779 (22) 15.6.1992  
 (71) TOSHIBA CORP (72) ATSUSHI SHINPO(3)  
 (51) Int. Cl.<sup>5</sup> H04L9/06, H04L9/14, H04K1/00

**PURPOSE:** To reduce the communication quantity by devising the method such that an authentication section authenticates only a radio terminal and a ciphering key between a base station and the radio terminal is shared in common.

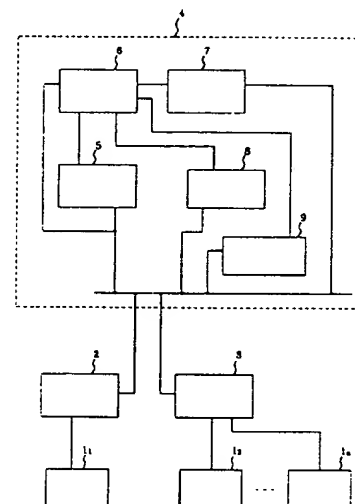
**CONSTITUTION:** A radio terminal sends an authentication number  $PS_i$  to a base station and the base station generates a random number  $R_1$  and sends it to the radio terminal. The radio terminal receives it to generate a random number  $R_2$ , an authentication information generating means 103 synthesizes the numbers  $R_1$ ,  $R_2$  and secret information  $S_{psi}$  to obtain an authentication number  $\sigma_{ps}$  and it is sent to the base station together with the random number  $R_2$ . The random numbers  $R_1$ ,  $R_2$ , the authentication number  $PS_i$  and the authentication number  $\sigma_{ps}$  are given to an authentication information check means 105, which authenticates the radio terminal as the terminal having the  $PS_i$  when the result of check is OK, and the radio terminal and the base station generate a common ciphering key by common share means 106a, 106b. Thus, a random number required for mutual authentication consists of key common share information and a function in the device to reduce number of random numbers to be converted thereby reducing the communication quantity.

**(54) STORAGE COMMUNICATION PROCESSING UNIT**

(11) 5-347618 (A) (43) 27.12.1993 (19) JP  
 (21) Appl. No. 4-155332 (22) 15.6.1992  
 (71) NIPPON TELEGR & TELEPH CORP <NTT>  
 (72) TOMOYOSHI HANEDA(1)  
 (51) Int. Cl.<sup>5</sup> H04L12/18, H04L12/54, H04L12/58

**PURPOSE:** To prevent the communication cost from being increased by not extending a line hold time to receive the communication result even when number of destinations of a multiple address call is increased.

**CONSTITUTION:** A destination number management equipment 6 stores a destination number corresponding to a call identification number given to a multiple address communication call by a call identification number provision device 5, stores the communication result to each destination number, and a communication information storage device 7 stores the communication information subject to multiple address communication. After the communication of the communication information is finished to destination information input output terminal equipments  $1_2, 1_3, \dots, 1_n$ , a communication result notice equipment 8 informs each destination number divided by each predetermined communication result to the information input output terminal equipment  $1_1$  of a multiple address communication sender. Moreover, when the noticed call identification number is inputted from the sender, an individual communication result notice equipment informs each destination number corresponding to the call identification number and the communication result to each destination number to the sender.



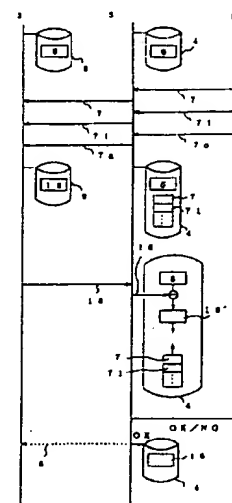
2,3: exchange, 4: store and forward communication processing unit, 9: individual communication result notice equipment

**(54) SETTING INFORMATION MANAGEMENT SYSTEM IN TRANSMITTER REMOTE CONTROL SYSTEM**

(11) 5-347619 (A) (43) 27.12.1993 (19) JP  
 (21) Appl. No. 4-155517 (22) 16.6.1992  
 (71) NEC CORP (72) DAISUKE TANIGUCHI  
 (51) Int. Cl.<sup>5</sup> H04L12/24, H04L12/26, H04M3/00

**PURPOSE:** To obtain the setting information management system in the transmitter remote control system in which the operability is not deteriorated even by a line setting revision instruction caused frequently.

**CONSTITUTION:** A line setting revision instruction of a transmitter 2 instructed from a network management system 1 by the operator is informed to the transmitter 2 from a transmitter control section 3 continuously for a prescribed time and revision setting information is stored in a data base 4. Then revision line setting information 16 being the entire information is read from the transmitter 2 after a lapse of a prescribed time, line setting information 5 before the continuous revision instruction, stored revision setting information 7 and the read revision line setting information 16 are compared to confirm whether or not the setting is correctly implemented. Thus, even in the case of the revision request caused frequently, the turnaround time is reduced and the deterioration in the operability is prevented.



(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平5-347617

(43)公開日 平成5年(1993)12月27日

(51)Int.Cl.<sup>5</sup>

識別記号

庁内整理番号

F I

技術表示箇所

H 0 4 L 9/06

9/14

H 0 4 K 1/00

Z 7117-5K

7117-5K

H 0 4 L 9/ 02

Z

審査請求 未請求 請求項の数 1 (全 18 頁)

(21)出願番号 特願平4-154779

(22)出願日 平成4年(1992)6月15日

(71)出願人 000003078

株式会社東芝

神奈川県川崎市幸区堀川町72番地

(72)発明者 新保 淳

神奈川県川崎市幸区小向東芝町1番地 株

式会社東芝総合研究所内

(72)発明者 尾林 秀一

神奈川県川崎市幸区小向東芝町1番地 株

式会社東芝総合研究所内

(72)発明者 鶴見 博史

神奈川県川崎市幸区小向東芝町1番地 株

式会社東芝総合研究所内

(74)代理人 弁理士 須山 佐一

最終頁に続く

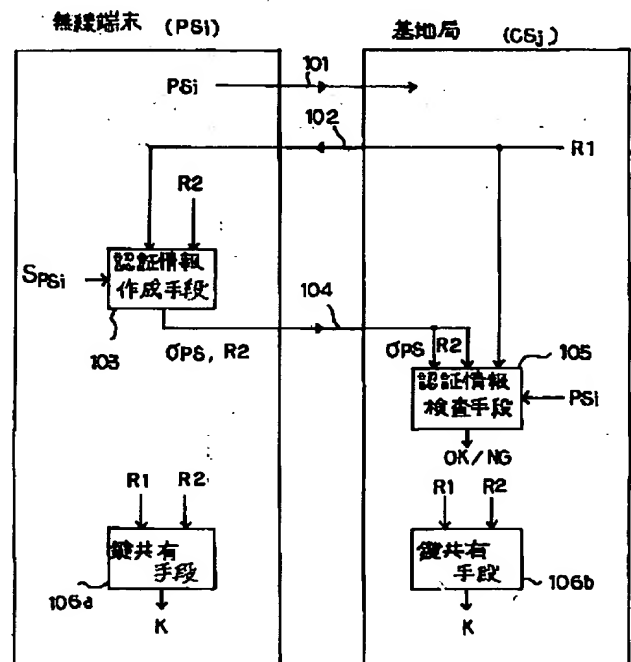
(54)【発明の名称】 無線通信システムの通信方法

(57)【要約】

【目的】 無線通信システムにおける無線端末の認証と基地局と無線端末間の暗号鍵の共有を通信量少なく実現することを目的とする。

【構成】 認証に必要な乱数情報を鍵共有情報として共用する。さらに、ランダム関数を用意し、この出力を乱数として扱うことにより、乱数情報の通信を減らす。

【効果】 鍵共有のために余分な通信がないこと、交換する乱数情報の数が減ることから通信量が少なくなる。



# 【特許請求の範囲】

【請求項1】 複数の無線端末と該無線端末からの通信情報を伝送・交換するネットワーク側装置としての複数の基地局および制御局から構成され、各無線端末は装置固有の第1の秘密情報と基地局の公開情報を有し、前記各基地局は、基地局の第2の秘密情報を有する無線通信システムであって、  
前記基地局が第1の乱数を生成して前記無線端末に送信する工程と、  
前記無線端末が第2の乱数を生成し、基地局の公開情報を用いて変換することにより鍵配送情報を生成し、前記第1の乱数と前記鍵配送情報と前記第1の秘密情報から認証情報を生成して鍵配送情報と認証情報を前記基地局に送信する工程と、  
前記基地局が、前記第1の乱数と前記鍵配送情報と前記認証情報が、所定の関係を満たすことを確認する工程と、  
前記基地局が前記第1の乱数と前記鍵配送情報と前記認証情報が、所定の関係を満たすことを確認すると、前記無線端末が前記第2の乱数と前記システムの公開情報から暗号鍵を求める工程と、  
前記基地局が、鍵配送情報と基地局の秘密情報から暗号鍵を求める工程と、を具備し、  
前記基地局が前記無線端末の正当性を確認することを特徴とする無線通信システムの通信方法。

## 【発明の詳細な説明】

### 【0001】

【産業上の利用分野】本発明は、端末の認証および通信内容の暗号化を要する自動車電話や携帯電話などの無線通信システムの通信方法に関する。

### 【0002】

【従来の技術】無線通信システムにおいては、有線系のシステムに比べ、通話内容の盗聴及び不正アクセスといった行為が容易となるため、これらを防止するためのセキュリティ対策が重要となる。具体的には、情報チャネルの暗号化及び無線端末の正当性の確認を行う必要が生じる。

【0003】このような無線通信システムのセキュリティを実現する方式は、次の点を満たすことが望ましい。

【0004】（1）無線端末の正当性の確認および基地局との間の無線回線の秘匿に必要な暗号鍵の共有のために必要な通信量が少ないこと。

【0005】（2）無線端末の正当性の確認は、基地局と無線端末の間のみで実行でき、かつ全無線端末に対応した情報を格納するデータベースは制御局に持たせ、基地局にはデータベースを置かないこと。

【0006】一般に認証や鍵共有のために伝送される情報は1ビットの誤りも許されない場合が多い。一方、基地局と無線端末の間の伝送路は無線回線であるため、誤り率が高い。誤り訂正符号の利用や誤り検出と再送手

順の組み合わせなどにより伝送路の誤り率を低くすることはできるが、一般に許容誤り率を小さく抑えることにより、伝送路のスループットが低下し、通話開始までに時間を要する。従って、認証や鍵共有のために伝送される情報は極力少なくする必要がある。これが（1）の要求項目である。

【0007】（2）は、発呼、着呼の度に生じる認証手順を簡略化する目的で必要となる。発呼、着呼の度に無線端末を認証するために制御局へのアクセスを必要とするのでは制御局への負荷の集中といった問題が生じる。一方、無線端末のデータベースを基地局に持たせる解決法が考えられるが、この場合には基地局の装置規模が大きくなることや基地局のデータベースの一貫性を保つために制御が複雑化することなどの問題が生じる。

【0008】さらに、将来、マイクロ・セル方式などによる基地局の小型化・セルの小ゾーン化が一層進み、多数の基地局が街頭に設置された状況を想定すると、基地局に対する物理的な攻撃も考慮する必要が生じる。物理的な攻撃とは、例えば、基地局の盗難・分解による基地局内秘密情報の漏洩や、基地局の複製などが挙げられる。このような状況では、次の要求項目が考えられる。

【0009】（3）基地局の分解あるいは基地局の複製という状況が生じて、無線端末の正当性確認に利用する秘密情報の漏洩は生じないこと。

【0010】無線端末の正当性確認に利用する秘密情報を取得した利用者は、本来の利用者に“なりすまし”で通信サービスを楽しむことができる。この“なりすまし”は、課金処理の根底を脅かすものであり、（3）を満たすことは必須条件となる。このような無線通信システムのセキュリティ機能を実現する場合、暗号技術を利用することが一般的である。以上の要求項目のうち、（2）と（3）は公開鍵暗号技術の利用により解決できる。

【0011】具体的には、例えばFiat-Shamir法で無線端末の正当性を確認できる。Fiat-Shamir法の詳細は、Fiat, A. and Shamir, A. “How to Prove Yourself: Practical Solutions to Identification and Signature Problems”, Proc. of CRYPTO’86, Lecture Notes on Computer Science 263, Springer-Verlag, pp. 186-194 に詳しくある。

【0012】しかしながら、Fiat-Shamir法を無線端末の認証に用いた場合、発呼（あるいは着呼）時の認証処理においては、正当な端末が確かに基地局にアクセスしたことが保証されるが、その認証処理終了後に不正端末が回線に割り込んで不正にアクセスする可能性が残る。

【0013】また、認証処理終了後、暗号鍵の共有を行い、以降の通信は共有された暗号鍵を用いて、メッセージ認証を行う方法が考えられるが、暗号鍵の共有手続きのために新たな通信が必要となる。暗号鍵の共有のために通信される情報も誤りが許されないため、通話開始ま

でに時間を要する原因となる可能性がある。

【0014】この問題点に対し、認証処理と暗号鍵共有処理を融合した構成が次の文献に提案されている：T. Okamoto and K. Ohta, "How to Utilize the Randomness of Zero-Knowledge Proofs", Proc. of CRYPTO'90. 認証処理で利用される乱数情報を鍵共有情報で構成していることがポイントである。提案されている方式の中で通信量が少ないものを次に示す。

【0015】文献の方式は、ユーザ1とユーザ2が相互に認証を行い、さらに暗号鍵の共有を行うものである。認証部分に拡張Fiat-Shamir 法による相手確認を用い、鍵共有部分にDH方式を用いている。

【0016】拡張Fiat-Shamir 法の詳細は、K. Ohta and T. Okamoto, "A Modification of the Fiat-Shamir Scheme" Proc. of CRYPTO'88 もしくは、L. C. Guillou and J. J. Quisquater, "A Practical Zero-Knowledge Protocol Fitted to Security Microprocessors Both Transmission and Memory", Proc. of EUROCRYPT'88. に詳しい。

【0017】また、DH鍵共有法の詳細は、W. Diffie and M. Hellman, "New Directions in Cryptography", IEEE Trans. IT-22, No. 6, pp. 644-654. に詳しい。

【0018】サービス提供者は素数  $p$ ,  $q$  を生成し、 $N = p \cdot q$  を公開の法の値とする。また、 $(p-1)$  および  $(q-1)$  と互いに素である整数  $e$  と公開の底の値  $g$  を定める。さらに、各ユーザに対し、次式を満たす秘密情報を求め、発行する。

【0019】

$$S_i = i / I_i \bmod N \quad (i = 1, 2, \dots)$$

但し、 $I_i$  はユーザ  $i$  の識別番号

処理手順は次の通りである。

【0020】(1) ユーザ1とユーザ2は互いに識別番号  $I_1$ ,  $I_2$  を交換する。

【0021】(2) ユーザ1は乱数  $r_1$  ( $1 < r_1 < N$ ) を生成し、次式により  $X_1$  を求め、これをユーザ2に送信する。

$$X_1 = g^{r_1} \bmod N$$

(3) ユーザ2は乱数  $r_2$  ( $1 < r_2 < N$ ) を生成し、次式により  $X_2$  を求める。

$$X_2 = g^{r_2} \bmod N$$

さらに、乱数  $E_1$  ( $1 < E_1 < e$ ) を生成し、 $E_1$  と  $X_2$  をユーザ1に送信する。

【0023】(4) ユーザ1は次式により、認証情報  $Y_1$  を計算する。

$$Y_1 = S_1^{E_1} \cdot g^{r_1} \bmod N$$

さらに、乱数  $E_2$  ( $1 < E_2 < e$ ) を生成し、 $E_2$  と  $Y_1$  をユーザ2に送る。

【0025】(5) ユーザ2は次式の検査を行う。

$$X_1 = ? Y_1^{E_2} \cdot I_1^{E_1} \bmod N$$

検査式が成立する場合には、ユーザ1を正当であると判

断する。

【0027】さらに、鍵  $K$  を次式により計算する。

$$K = X_1^{r_2} \bmod N = g^{r_1 \cdot r_2} \bmod N$$

また、認証情報  $Y_2$  を次式により計算し、ユーザ1に送信する。

$$Y_2 = S_2^{E_2} \cdot g^{r_2} \bmod N$$

(6) ユーザ1は次式の検査を行う。

$$X_2 = ? Y_2^{E_1} \cdot I_2^{E_2} \bmod N$$

検査式が成立する場合には、ユーザ2を正当であると判断する。さらに、鍵  $K$  を次式により計算する。

$$K = X_2^{r_1} \bmod N = g^{r_1 \cdot r_2} \bmod N$$

上記手順によれば、認証処理を行い、その正当性が確認された場合のみ鍵共有を行うことができる。鍵共有のために新たに通信を必要とすることはない。しかしながら、この方式は、不特定多数の通信者間の鍵生成を、平等に行うために設計されたものであり、相互の認証を行っている。実際の無線端末と基地局の間では、例えば無線端末の認証は必要とされるが基地局の認証は必要としない場面が多い。また、上記手順では ( $X_1$ ,  $E_1$ ,  $Y_1$ ,  $X_2$ ,  $E_2$ ,  $Y_2$ ) の通信が必要であり、仮に法  $N$  のサイズを512ビットとし、 $e$  のサイズを64ビットとすると全通信量は2176ビットとなり、通信量がやや多い。なお、この通信量には、識別番号  $I_1$ ,  $I_2$  の通信は含んでいない。識別番号の通信は、認証処理以前に送信されるものと考えられるからである。

【0032】

【発明が解決しようとする課題】以上述べてきたように、従来技術による端末の正当性確認を無線通信システムに適用した場合、正当な無線端末が認証された後で、不正端末がその回線に割り込んでアクセスする可能性があった。これを防止する方法として、無線端末の認証と暗号鍵の共有を同時に実現する方式も存在するが、対等な2者間での相互認証・鍵共有を前提としているため、通信量が多いことが欠点であった。

【0033】本発明の目的は、認証部分では無線端末の認証のみを行い、これと基地局—無線端末間の暗号鍵の共有を同時に実現する方式を提供するとともに、基地局—無線端末の相互認証と暗号鍵の共有を同時に実現する方式であって、従来よりも通信量の少ない方式を提供することにある。

【0034】

【課題を解決するための手段】前述した目的を達成するために、本発明は複数の無線端末と該無線端末からの通信情報を伝送・交換するネットワーク側装置としての複数の基地局および制御局から構成され、各無線端末は装置固有の第1の秘密情報とシステムの公開情報を有し、前記各基地局は、基地局の第2の秘密情報を有する無線通信システムであって、前記基地局が第1の乱数を生成して前記無線端末に送信する工程と、前記無線端末が第2の乱数を生成し、基地局の公開情報を用いて変換する

ことにより鍵配送情報を生成し、前記第1の乱数と前記鍵配送情報と前記第1の秘密情報から認証情報を生成して前記基地局に送信する工程と、前記基地局が、前記第1の乱数と前記鍵配送情報と前記認証情報が、所定の関係を満たすことを確認する工程と、前記基地局が前記第1の乱数と前記鍵配送情報と前記認証情報が、所定の関係を満たすことを確認すると、前記無線端末が前記第2の乱数と前記基地局の公開情報から暗号鍵を求める工程と、前記基地局が、鍵配送情報と基地局の秘密情報から暗号鍵を求める工程と、を具備し、前記基地局が前記無線端末の正当性を確認することを特徴とする無線通信システムの通信方法である。

#### 【0035】

【作用】本発明は、基地局による無線端末の認証と鍵共有を融合した方式である。各無線通信端末には、自装置固有の秘密情報と基地局の公開情報が発行される。一方、基地局には、基地局の秘密情報が発行される。認証は次の手順で行う。まず、基地局が第1の乱数を生成し、無線端末に送信する。無線端末は、第2の乱数を生成し、これを基地局の公開情報で暗号化して鍵配送情報を生成する。さらに、無線端末は第1の乱数と鍵配送情報に対し、自装置の秘密情報を作用させ認証情報を作成し、鍵配送情報と認証情報を基地局に送信する。基地局は、第1の乱数と鍵配送情報と認証情報が所定の関係式を満たすことを確認することによって無線端末の認証を行う。認証後に、基地局は認証時の鍵配送情報と基地局の秘密情報から暗号鍵を得る。一方、無線端末は、第1の乱数と基地局の公開情報から暗号鍵を得る。

【0036】さらに、基地局による無線端末の認証と鍵共有を融合することもできる。この場合、無線端末と基地局には、それぞれ、通信相手の識別番号により共有情報を出力する鍵共有関数を発行しておく。この鍵共有関数はそれぞれの装置ごとに異なる。また、各無線端末には自装置固有の秘密情報を発行しておく。基地局による無線端末の認証は、次の手順で行う。基地局と無線端末が共に乱数を生成する。無線端末は、この2種類の乱数に秘密情報を作用させて認証情報を生成する。基地局は、前記2種類の乱数と認証情報が所定の関係式を満たすことを確認することで行う。これが確認された場合に、認証時に交換した情報と相手識別番号により無線端末と基地局が暗号鍵を共有する。認証時に交換した情報を鍵共有関数の入力の一つとすることにより、共有される鍵の値が毎回変わり、認証処理と鍵共有処理が連結される。

【0037】また、無線端末と基地局の相互認証と鍵共有を融合することもできる。この場合、無線通信端末および基地局には、それぞれ自装置固有の秘密情報を発行しておく。さらに各々の装置に共通の乱数生成関数を備える。無線端末と基地局が相互に正当性を確認する手順を次の考え方のもとに行う。基地局と無線端末は、相互

の鍵共有に必要な鍵共有情報を作成し、これを相互に通信する。相互認証時に必要な乱数は、前記鍵共有情報と乱数生成関数から生成する。相互の装置の正当性が確認された場合に前記鍵共有情報から共通の暗号鍵を生成する。相互認証に必要な乱数を鍵共有情報と装置内の関数から構成するために、通信により交換する乱数の数を減らすことができ、通信量の削減になる。

#### 【0038】

【実施例】以下、図面を参照して本発明の実施例を説明する。

【0039】まず、無線通信システムの構成を図2に示す。無線端末には、それぞれ固有の識別番号(PSi)が与えられ、さらに固有の秘密情報( $S_{PSi}$ )が発行される。ネットワーク側は、制御局CCと複数の基地局CS<sub>1</sub>、…CS<sub>n</sub>からなる。全基地局には共通の基地局秘密情報が発行される。制御局CCには、各々の無線端末に対する課金情報などを蓄積したデータベースが存在する。基地局CS<sub>i</sub>にはデータベースは存在しない。基地局CS<sub>i</sub>と無線端末PS<sub>i</sub>間の通信は、無線が利用されるが、基地局CS<sub>i</sub>と制御局CCの間の通信は、有線もしくは無線である。無線端末PS<sub>i</sub>の正当性の確認および無線回線で用いる暗号方式用の暗号鍵の共有は、無線端末PS<sub>i</sub>と基地局CS<sub>i</sub>の間で行われ、中央の制御局CCにアクセスする必要はない。このような認証方式が実行されるのは、無線端末PS<sub>i</sub>からの発信時、別の無線端末PS<sub>j</sub>への着信時などである。

【0040】図1に本発明による無線端末の認証・鍵共有方式を示す。

【0041】(1)無線端末から基地局へ、無線端末の識別番号PSiが送信される。

【0042】…(ステップ101)

(2)基地局は、第1の乱数R1を生成し、無線端末に送信する。

【0043】…(ステップ102)

(3)無線端末は、第2の乱数R2を生成し、R1とR2と秘密情報 $S_{PSi}$ とを認証情報作成手段103により合成し、認証情報 $\sigma_{PS}$ を得る。

【0044】…(ステップ103)

認証情報 $\sigma_{PS}$ と第2の乱数R2を基地局に送信する。…

(ステップ104)

(4)基地局は、第1の乱数R1と第2の乱数R2と無線端末の識別番号PSiと認証情報 $\sigma_{PS}$ を認証情報検査手段105に通し、結果がOKの場合には、無線端末をPSiであるものと認証する。結果がNGの場合には、不正端末であるとして、処理を終了する。

…(ステップ105)

(5)上記認証処理に成功した場合、無線端末と基地局は、共通の暗号鍵を鍵共有手段106a、106bにより生成する。このとき、新たに情報の交換を行わず、上記認証処理で交換した情報および自装置内に予め格納さ

れていた情報のみを利用する。

… (ステップ106)

上記手順のうち、(2)から(4)の無線端末の正当性確認部分は、ID情報に基づく相手確認法あるいは、ID情報に基づくデジタル署名法を利用したチャレンジ・レスポンス方式で構成する。このような方法で構成することの利点として次のことが挙げられる。

①基地局側に必要な情報は、無線端末の識別番号と基地局の公開情報、基地局の秘密情報のみであり、基地局が分解されても無線端末の秘密情報は存在しない。さらに、通信情報から無線端末の秘密情報は漏洩しない。従って、無線回線上の情報の盗聴やニセ基地局相手に認証処理を行った場合にも安全性が確保できる。無線端末の作用させる乱数が秘密情報の漏洩を防ぐ。

【0045】②互いの装置が毎回乱数を作用させるので、ある時点で正当な無線端末から送信された認証情報を通信回線上で盗み、それを再送したとしても、認証処理を通過できない。

【0046】③①で指摘したように、認証時に相手装置の識別番号の送信が必要となるが、この情報は、認証処理以前に送信される可能性があるため、通信量が削減できる。ID情報に基づく方式でないデジタル署名方式(例えばRSA暗号など)を利用する場合には、無線端末固有の公開情報とその正当性証明情報(KohnfelderによるPublic Key Certificateなど)の送信が必要であり、その分通信量が増加する。

【0047】ID情報に基づく相手確認法およびデジタル署名法の具体例には、次の方式がある。

【0048】・Fiat-Shamir法: A Fiat and A. Shamir, "How to Prove Yourself", Proc. of CRYPTO'86.

・拡張Fiat-Shamir法: K. Ohta and T. Okamoto, "A Modification of the Fiat-Shamir Scheme", Proc. of CRYPTO'88.

もしくは、L. C. Guillou and J. J. Quisquater, "A Practical Zero-Knowledge Protocol Fitted to Security Microprocessors Both Transmission and Memory", Proc. of EUROCRYPT'88.

・拡張Fiat-Shamir法2: 太田和夫, "RSA暗号を利用したIDに基づく認証方式とその応用", 第11回情報理論とその応用シンポジウム予稿集, pp. 567-572.

・Beth法: T. Beth, "Efficient Zero-Knowledge Identification Scheme for Smart Cards", Proc. of EUROCRYPT'88.

上記の中で通信量が少なく、無線端末システムの認証に適する方式として、拡張Fiat-Shamir法1と2が挙げら\*

$$R2 = g^r \text{ mod } N$$

$$X = R2^e \text{ mod } N$$

$$E = h(X, R1)$$

$$\sigma_{PS} = S_{PSi}^E \cdot R2 \text{ mod } N$$

認証情報 $\sigma_{PS}$ およびEを基地局に送信する。

\*れる。以降の実施例では、拡張Fiat-Shamir法1による相手確認法およびデジタル署名法を認証部分に利用している。

【0049】図1の手順(5)の鍵共有処理では、余分な通信を必要としないため、全体の通信量は、(2)から(4)の認証部分の通信量に等しい。認証部分の通信量は、通常の相手確認の通信量と同じであるので、全体の通信量が少ない。

【0050】図3には、認証手順を拡張Fiat-Shamir法による署名により実現し、鍵共有手順をDH鍵共有法により実現した実施例を示す。

【0051】まず、サービス提供者は次の準備を行う必要がある。まず、2つの素数 $p, q$ を定め、その積を $N$ とする。また、 $(p-1)$ と $(q-1)$ の最小公倍数を $L$ とし、 $L$ と互いに素である整数 $e$ を定める。さらに、 $GF(p), GF(q)$ で共に原始根となる整数 $g$ を定める。また、基地局の秘密情報 $t$  ( $1 < t < L$ )を定め、基地局の公開鍵 $G$ を

$$G = g^t \text{ mod } N$$

で求める。無線端末 $PSi$ に対しては、次式を満たす秘密情報 $S_{PSi}$ を求め、秘密に発行する。

$$【0052】 S_{PSi}^e = PSi \text{ mod } N$$

但し、 $PSi$ は無線端末 $PSi$ の識別番号

さらに、一方向性の圧縮関数 $h()$ を定める。例えば、ブロック暗号DES(Data Encryption Standard)のCBCモードで構成した関数を $h()$ とする。

【0053】以上で生成した情報を次のように管理する。

①基地局の公開情報(全無線端末と全基地局に発行する):  $N, g, G, e, h()$

②基地局の秘密情報(全基地局に発行する):  $t$

③無線端末の秘密情報(無線端末 $PSi$ に発行する):  $S_{PSi}$

$PSi$

④サービス提供者の秘密情報:  $p, q, L$

処理の手順は次のようになる。

【0054】(1)無線端末は、基地局に自装置の識別番号 $PSi$ を送信する。

【0055】… (ステップ301)

(2)基地局は、第1の乱数 $R1$  ( $1 < R1 < N$ )を生成し、 $R1$ を無線端末に送信する。

… (ステップ302)

(3)無線端末は、乱数 $r$  ( $1 < r < N$ )を生成し、次式の計算を実行する。

【0056】

… (ステップ303)

(ステップ304)

(4) 基地局は、次式の計算を行う。

$$【0057】 X' = \sigma_{PS} / \text{PSi}^E \bmod N$$

無線端末から送信されたEと次式の右边が一致するかど

$$E = ? h(X', R1)$$

… (ステップ305)

(5) 基地局は、(4)において無線端末の正当性を確認した場合、次の計算により暗号鍵Kを求める。

$$K = X'^t \bmod N = g^{t \cdot r} \bmod N \quad \dots (\text{ステップ306})$$

一方、無線端末は、次の計算により暗号鍵Kを求める。

$$K = G^r \bmod N = g^{r \cdot t} \bmod N \quad \dots (\text{ステップ307})$$

上記方式の鍵共有方式では、離散対数問題 ( $G = (g^t)^r \bmod N$  の値から  $t$  の値を求めること。もしくは、 $X = (g^r)^t \bmod N$  の値から  $r$  の値を求めること) が困難である限り、第三者は暗号鍵の値を求められない。

【0061】 上記方式の通信量は、法Nのサイズを512ビット、一方向性関数hの出力を64ビット、乱数R1を64ビットと仮定すると、640ビットである。

【0062】 図4には、認証手順を拡張Fiat-Shamir法の署名方式で実現し、さらに、無線端末と基地局の安全な装置構成を前提とした鍵共有方式による実施例を示す。

【0063】 (1) 無線端末は、基地局に自装置の識別番号PSiを送信し、基地局は、無線端末に自装置の識別番号CSjを送信する。

… (ステップ401)

(2) 基地局は、乱数R1 ( $1 < R1 < N$ ) を生成し、★

$$E = ? h(X', R1)$$

(5) 基地局は、(4)において無線端末の正当性を確認した場合、自装置内の関数  $f_{CSj}$  に無線端末の識別番号PSiと乱数R1とX'を入力して共有鍵Kを求める。

… (ステップ406)

6)

一方、無線端末は、自装置内の関数  $f_{PSi}$  に基地局の識別番号CSjと乱数R1とXを入力して共有鍵Kを求める。

… (ステップ407)

なお、乱数R1とX (あるいはX') を利用する代わりにEを入力するようにしてもよい。

【0067】 上記方式の通信量は、図3に示す実施例と同様640ビットである。

【0068】 図4に示す実施例において(4)の鍵共有部で利用する関数  $f_{PSi}$  (501) と  $f_{CSj}$  (502) の一例を図5に示す。図5における関数  $f$  (503) は秘密であり、多入力の関数である。無線端末の識別番号PSi (504) と基地局の識別番号CSj (505)、さらに認証処理で使用された乱数情報 (506) を入力する構成である。これらの乱数情報の入力により、認証処理ごとに異なる鍵K (507) が共有される。無線端末側の関数  $f_{PSi}$  は、自装置の識別番号PSiの関数  $f$  への入力を変更できないように装置構成されている。すなわち、PSiの入力 (504) の部分に、他の無線端末の識別番号PSjを入力することができないように構成されている。基地局側の関数  $f_{CSj}$  も同様に、自装置の識別番号CSjが変更できないように装置構成さ

\* うか確認する。

$$【0058】$$

※ 【0059】

★無線端末に送信する。

$$【0064】 \dots (\text{ステップ402})$$

(3) 無線端末は、乱数R2 ( $1 < R2 < N$ ) を生成し、次式の計算を実行する。

$$X = R2^E \bmod N$$

$$E = h(X, R1)$$

$$\sigma_{PS} = S_{PSi}^E \cdot R2 \bmod N \quad \dots$$

(ステップ403)

認証情報  $\sigma_{PS}$  およびEを基地局に送信する。

(ステップ404)

(4) 基地局は、次式の計算を行う。

$$20 \quad 【0065】 X' = \sigma_{PS} / \text{PSi}^E \bmod N$$

無線端末から送信されたEと次式の右边が一致するかどうか確認する。

$$【0066】$$

… (ステップ405)

れる。このように構成することにより、不正端末が無線端末PSiと基地局CSjの間の鍵を共有することが不可能になる。

【0069】 このような装置構成により暗号鍵の共有部分を実現した場合、その装置構成を破られると鍵共有の安全性は保証されない。しかし、このことは、認証部分の安全性には、影響しない。

【0070】 次に、基地局と無線端末が相互に認証を行いながら、鍵共有を行う方式の実施例を説明する。この場合には、基地局にも、それぞれ固有の秘密情報  $S_{CSj}$  が発行される。

【0071】 図6に無線端末と基地局の相互認証・鍵共有方式の一基本構成を示す。

【0072】 (1) 無線端末から基地局へ、無線端末の識別番号PSiが送信される。また、基地局から無線端末へ、基地局の識別番号CSjが送信される。

【0073】 … (ステップ601)

(2) 基地局は、第1の乱数R1を生成し、無線端末に送信する。

【0074】 … (ステップ602)

(3) 無線端末は、第2の乱数R2を生成し、R1とR2と秘密情報  $S_{PSi}$  とを認証情報作成手段により合成し、認証情報  $\sigma_{PS}$  を得る。

【0075】 … (ステップ603)

50 この認証情報  $\sigma_{PS}$  と第2の乱数R2を基地局に送信す

る。

【0076】… (ステップ604)

(4) 基地局は、R1とR2と無線端末の識別番号PSiと認証情報 $\sigma_{PS}$ を認証情報検査手段に通し、結果がOKの場合には、無線端末をPSiであるものと認証する。結果がNGの場合には、不正端末であるとして、処理を終了する。

… (ステップ605)

さらに、R1とR2と秘密情報 $S_{CSj}$ とを認証情報作成手段により合成し認証情報 $\sigma_{CS}$ を得る。

… (ステップ606)

この認証情報 $\sigma_{CS}$ を無線端末に送信する。

(ステップ607)

(5) 無線端末は、R1とR2と基地局の識別番号CSjと認証情報 $\sigma_{CS}$ を認証情報検査手段に通し、結果がOKの場合には、基地局をCSjであるものと認証する。結果がNGの場合には、不正基地局であるとして、処理を終了する。

… (ステップ608)

(6) 上記認証処理に成功した場合、無線端末と基地局は、共通の暗号鍵を鍵共有手段により生成する。このとき、新たに情報の交換を行わず、上記認証処理で交換した情報および自装置内に予め格納されていた情報のみを利用する。

… (ステップ609)

この手順は、図1の基本構成を双方向にしたものである。図1の基本構成では、無線端末のみの認証を行う目的で、乱数を基地局と無線端末のそれぞれが生成し、相手装置に送信していた。上記手順では、相互の認証を行う目的に対して、無線端末の認証のみを行う場合と同数の乱数を利用することにとどめている。このときに不足する乱数を補うために、一方向性のランダム関数を全装置に備えておき、相手装置からの送信情報をランダム関数に作用させた結果を利用する。通信により交換する乱数が少なくなる分、通信量が減少する。 \*

$$R1 = g^{r1} \bmod N$$

$$X1 = R1^* \bmod N$$

X1を無線端末に送信する。

(ステップ703)

(3) 無線端末は、乱数 $r2$  ( $1 < r2 < N$ ) を生成 ※40

$$R2 = g^{r2} \bmod N$$

$$X2 = R2^* \bmod N$$

X2を基地局に送信する。

(ステップ705)

(4) 基地局は、関数 $h$ にX2を入力することにより、E1を得る。 ★

$$Y_{CS} = S_{CSj}^{E1} \cdot R1 \bmod N$$

認証情報 $Y_{CS}$ を無線端末に送信する。

(ステップ707)

(5) 無線端末は、基地局CSjの正当性を次式の計算・

\* 【0077】図7には、拡張Fiat-Shamir法による相手確認による相互認証とDH法による鍵共有法を融合した実施例を示す。

【0078】まず、サービス提供者は次の準備を行う必要がある。まず、2つの素数 $p$ 、 $q$ を定め、その積を $N$ とする。また、 $(p-1)$ と $(q-1)$ の最小公倍数を $L$ とし、 $L$ と互いに素である整数 $e$ を定める。さらに、 $GF(p)$ 、 $GF(q)$ で共に原始根となる整数 $g$ を定める。無線端末PSiに対しては、次式を満たす秘密情報 $S_{PSi}$ を求め、秘密に発行する。

$$【0079】 S_{PSi}^* = PSi \bmod N$$

但し、PSiは無線端末PSiの識別番号

また、基地局CSjに対しても同様に次式を満たす秘密情報 $S_{CSj}$ を求め、秘密に発行する。

$$【0080】 S_{CSj}^* = CSj \bmod N$$

但し、CSjは基地局CSjの識別番号

さらに、一方向性の圧縮関数 $h()$ を定める。例えば、ブロック暗号DES(Data Encryption Standard)のCBCモードで構成した関数を $h()$ とする。

【0081】以上で生成した情報を次のように管理する。

【0082】①システムの公開情報(全無線端末と全基地局に発行する) :  $N, g, e, h()$

②基地局の秘密情報(基地局CSjに発行する) :  $S_{CSj}$

③無線端末の秘密情報(無線端末PSiに発行する) :  $S_{PSi}$

④サービス提供者の秘密情報 :  $p, q, L$

処理手順は次の通り。

【0083】(1) 無線端末から基地局へ識別番号PSiが送信される。一方、基地局から移動端末へ識別番号CSjが送信される。 … (ステップ701)

(2) 基地局は、乱数 $r1$  ( $1 < r1 < N$ ) を生成し、次式の計算を行う。

$$【0084】$$

… (ステップ702)

※し、次式の計算を行う。

$$【0085】$$

… (ステップ704)

★ 【0086】  $E1 = h(X2)$

このE1と秘密情報 $S_{CSj}$ 、R1とから次式の計算を行う。

$$【0087】$$

… (ステップ706)

検査により行う。

$$【0088】$$

$$E1 = h(X2)$$



$$Y_{cs} = ? CS_j^{E1} \cdot X1 \bmod N$$

この関係式が成立した場合には、基地局を正当であると判断する。

【0089】… (ステップ708)

$$E2 = h(Y1)$$

$$Y_{rs} = S_{PSi}^{E2} \cdot R2 \bmod N$$

認証情報  $Y_{rs}$  を基地局に送信する。

(ステップ710)

$$K = X1^{r2} \bmod N$$

$$= g^{e \cdot r1 \cdot r2} \bmod N$$

(6) 基地局は、無線端末  $PSi$  の正当性を次式の計算・検査により行う。

【0092】

$$E2 = h(Y1)$$

$$Y_{cs} = ? PSi^{E2} \cdot X2 \bmod N$$

$$K = X2^{r1} \bmod N$$

$$= g^{e \cdot r1 \cdot r2} \bmod N$$

上記方式の、ステップ702, 706, 708 は、基地局の正当性に対する拡張Fiat-Shamir の相手確認法とみなすことができる。この中で  $X2$  を相手確認に利用する検証者の乱数情報とみなしている。一方、ステップ704, 709, 712

は、無線端末の正当性に関する拡張Fiat-Shamir の相手確認法とみなすことができる。この中で、 $Y_{cs}$  を検証者乱数情報とみなしている。 $Y_{cs}$  の値は、ステップ707 の時点まで無線端末には予測ができないので、こうした利用が可能である。なお、上記方式では、基地局が先にその正当性を証明する手順であるが、逆に無線端末が先に正当性を証明する手順にしてもよい。

【0095】上記方式は、従来技術の項に記述した岡本一太田による鍵共有法とほぼ同様の手順であるが、上記方式の特徴は、検証者の乱数  $E1$ 、 $E2$  をそれぞれ  $X2$ 、 $Y1$  (前記手順では  $Y_{cs}$ ) から生成するようにしている点である。このことにより、 $E1$ 、 $E2$  の伝送が ☆

$$R1 = g^{r1} \bmod N$$

$$X1 = R1^e \bmod N$$

$X1$  を無線端末に送信する。

(ステップ803)

(3) 無線端末は、乱数  $r2$  ( $1 < r2 < N$ ) を生成 ◆

$$R2 = g^{r2} \bmod N$$

$$X2 = R2^e \bmod N$$

$$E2 = h(X1, X2)$$

$$Y_{rs} = S_{PSi}^{E2} \cdot R2 \bmod N$$

$Y_{rs}$  と  $E2$  を基地局に送信する。

(ステップ805)

(4) 基地局は、次の手順により無線端末の認証を行う。

【0102】

$$X2' = Y_{rs} / PSi^{E2} \bmod N$$

$$E2 = ? h(X1, X2')$$

$$E1 = h(Y_{rs})$$

\* 検査が成功した場合、次式により認証情報  $Y_{rs}$  を計算する。

【0090】

… (ステップ709)

※ さらに、暗号鍵  $K$  を次式の計算により求める。

【0091】

… (ステップ711)

★ この関係式が成立した場合には、無線端末を正当であると判断する。

【0093】… (ステップ712)

さらに、暗号鍵  $K$  を次式の計算により求める。

【0094】

… (ステップ713)

☆ 要となっている。 $E1$ 、 $E2$  も伝送誤りの許されない情報であることから、無線通信システムの認証・鍵共有では、前記図7の手順の方が通信量の少ない分だけ有効となる。

【0096】上記方式の通信量は、法  $N$  のサイズを512ビットと仮定すると、2048ビットである。

【0097】図8には、拡張Fiat-Shamir 法によるデジタル署名と相手確認をそれぞれの認証方式に利用し、鍵共有方式にDH方式を利用した実施例を示す。

【0098】処理手順は次の通り。

【0099】(1) 無線端末から基地局へ識別番号  $PSi$  が送信される。一方、基地局から移動端末へ識別番号  $CSj$  が送信される。

… (ステップ801)

(2) 基地局は、乱数  $r1$  ( $1 < r1 < N$ ) を生成し、次式の計算を行う。

【0100】

… (ステップ802)

◆ し、次式の計算により認証情報  $Y_{rs}$  を求める。

【0101】

… (ステップ804)

この関係式が成立した場合には、無線端末を正当であると判断する。

【0103】… (ステップ806)

検査に通った場合、次式により認証情報  $Y_{cs}$  を計算する。

【0104】

15

$$Y_{cs} = S_{csj}^{e1} \cdot R1 \bmod N$$

認証情報  $Y_{cs}$  を無線端末に送信する。

(ステップ808)

$$K = X2^{r1} \bmod N = g^{e \cdot r1 \cdot r2} \bmod N$$

(5) 無線端末は、基地局CSjの正当性を次式の計算・検査により行う。

【0106】

$$E1 = h(Y_{ps})$$

$$Y_{cs}^* = ? CSj^{e1} \cdot X1 \bmod N$$

$$K = X1^{r2} \bmod N = g^{e \cdot r1 \cdot r2} \bmod N$$

図8の手順において、ステップ804の $Y_{ps}$ は、 $X1$ に対する拡張Fiat-Shamir署名となっている。一方、ステップ802の $X1$ とステップ807の $Y_{cs}$ は、拡張Fiat-Shamirの相手確認法となっているとみなすことができる。このとき、 $Y_{ps}$ の値は基地局にとって予測できないものであり、これを相手確認法における乱数として利用している。

【0109】上記方式の通信量は、法Nのサイズを512ビット、一方向性関数hの出力値を64ビットと仮定すると、1600ビットである。

【0110】次に、無線端末PSiが、制御局CCによって自分の公開鍵と無線端末のIDに関してなされたデジタル署名をされたものを、基地局CSに送信し、基地局CSがこれを無線端末PSの認証に用いることで、不正使用を防止する方式について述べる。

【0111】図9において、制御局CCで、無線端末PSiの公開鍵 $Kei$ 及びPSiのID番号 $Idi$ に対して、制御局CCの秘密鍵 $Kdcc$ によって署名を行う。署名の結果 $S1$ をあらかじめ無先端末PSiに持たせる。

【0112】無線端末PSiは、認証開始時に、自らのID番号 $Idi$ と上記の署名の結果 $S1$ を、基地局CSiに送信する。あらかじめ制御局CCの公開鍵 $Kecc$ を記憶している基地局CSiは、署名の結果、 $S1$ を公開鍵 $Kecc$ で検査を行い、出力された結果のうち、ID番号にあたる部分が無線端末PSiのID番号 $Idi$ と同一か否かを比較する。この比較により、先の検査の出力結果のうち残りの公開鍵の部分を無線端末PSiの公開鍵 $Kei$ と認識する。

【0113】次に、基地局CSiはあるメッセージMを無線端末PSiに送出する。受信した無線端末PSiは、メッセージMに対してハッシュ関数を用いて圧縮処理した結果に対して、無線端末PSiの秘密鍵 $Kdi$ を用いて署名を行う。署名結果 $S2$ を基地局CSiへ送出する。CSiは、署名結果 $S2$ を先の検査で出力された無線端末PSiの公開鍵 $Kei$ を用いて検査する。この検査結果を、メッセージMに対して無線端末PSiと同一のハッシュ関数で圧縮処理した結果と比較し、認証に用いることで、不正使用を防止することができる。

【0114】ここで、単純化のためハッシュ関数による

16

… (ステップ807)

\* さらに、暗号鍵Kを次式の計算により求める。

【0105】

… (ステップ809)

※この関係式が成立した場合には、基地局を正当であると判断する。

【0107】… (ステップ810)

さらに、暗号鍵Kを次式の計算により求める。

【0108】

… (ステップ811)

双方での圧縮処理を省略することも考えられる。また、無線端末PSiに関する認証を考えたが、契約している無線端末の利用者に関する認証に関しても、パーソナルIDの入ったICカードを無線端末に挿入などの作用をすることにより、同様の効果を得ることができる。以下の実施例でも同じことが言える。

【0115】本実施例に拠れば、制御局CC側に公開鍵のDBを持たせたり、制御局CCにアクセスすることなく、公開鍵による認証を行うことができる。したがって、マイクロセル方式を用いた場合に飛躍的に増大する基地局CSと制御局CCや交換機などの間でやりとりされる情報量を極力減らすことができる。

【0116】一方、マイクロセル方式では基地局CSは小形になり、設置場所も従来のビルの屋上などから、建物の壁の低い位置など一般の通行人の目に触れやすい場所になり、盗難の恐れが増える。また、一部は、電池駆動になったり、制御局とのリンクを無線で張ったりすることが考えられ、この場合は、盗難の恐れがさらに増大し、盗難された時の悪意を持った改造がより簡単になる恐れがある。しかし、本実施例に拠れば、基地局CSが盗難されたとしても、慣用暗号を用いた認証のために用いる秘密鍵をROMなどから読み出された場合に比べ、偽の認証データの捏造や悪用の可能性は極めて低くなる。

【0117】また、慣用暗号を用いた認証を採用した場合、悪意をもって偽の基地局CSを構成し、通話開始前の認証用情報のやり取りから、端末に記憶されている秘密鍵などの秘密情報を吸い上げてしまう行為を許してしまう可能性がある。しかし、公開鍵暗号を用いた本実施例に拠れば、このような行為を許す可能性はなくなる。

さらに、複数のサービス提供者の間で、相互ハンドオフサービスを行う場合、ハンドオフの際にあらためて認証を必要とする可能性がある。このときも、制御局側にアクセスすることなく認証が行えるため、ハンドオフにかかる時間の短縮化にも寄与する。

【0118】加えて、無線端末PSによる基地局CSの認証にも同様の手続きを適用することも考えられる。

【0119】図10に示す実施例は、片方向のみの送受信を用いることで、認証に要する時間の低減を図ったものである。

20

30

40

50

【0120】前半の署名の結果 $S_1$ とID番号 $ID_i$ の伝送にかかわる処理は、図9に示す実施例と同様である。

【0121】次に、無線端末 $PS_i$ はあるメッセージ $M$ に対してハッシュ関数を用いて圧縮処理した結果に対して、無線端末 $PS_i$ の秘密鍵 $K_{di}$ を用いて署名を行う。署名結果 $S_2$ とメッセージ $M$ を基地局 $CS_i$ へ送出する。基地局 $CS_i$ は、署名結果 $S_2$ を先の検査で出力された無線端末 $PS_i$ の公開鍵 $K_{ei}$ を用いて検査する。この検査結果、メッセージ $M$ に対して無線端末 $PS_i$ と同一のハッシュ関数で圧縮処理した結果と比較し、

認証に用いることで、不正使用を防止することができる。

【0122】ここで、単純化のためハッシュ関数による双方での圧縮処理を省略することも考えられる。

【0123】本実施例では、署名結果 $S_2$ とメッセージ $M$ との送出を連続して行い、署名結果 $S_2$ の処理とメッセージ $M$ の送出を時間的に並列に行うことができるため、認証に要する時間が低減できる。

【0124】ただし本実施例では、片方向のみの伝送が行われるため、この一連の伝送の履歴を盗聴された場合に、同一手順を踏むことによって認証手続きが破られる恐れがある。しかし、メッセージ $M$ に現在の年月日および時刻を用いることなどによって、ある程度の安全性を与えることができる。

【0125】図11に示す実施例では、認証に要する情報（以下、これを認証用情報と称する）を、適当な長さのバーストに分割し、個々のバーストについて自動再送手順を用いるものである。

【0126】図12、図13に、仮定する2種類のバースト構成を示す。

【0127】図12に示すバーストは、過渡応答用ランブタイム $R$ （4ビット）、スタートシンボル $SS$ （2ビット）、プリアンブル $PR$ （6ビット）、同期ワード $UW$ （16ビット）、情報ビット $I$ （196ビット）と16ビットのガードビットからなる。情報ビット $I$ は、図12（b）に示すように、チャンネル種別 $CI$ （4ビット）、低速付随制御チャンネル $SA$ （16ビット）、トラヒックチャンネル $TCH$ （160ビット）、CRC（16ビット）からなる。

【0128】図13に示すバーストは、過渡応答用ランブタイム $R$ （4ビット）、スタートシンボル $SS$ （2ビット）、制御信号 $CAC$ （62ビット）、同期ワード $UW$ （32ビット）、制御信号 $CAC$ （124ビット）と16ビットのガードビットからなる。62ビットの制御信号 $CAC$ は、図13（b）に示すユーザ特定制御チャンネル $USCCH$ であり、124ビットの制御信号 $CAC$ は、チャンネル識別 $CI$ （4ビット）、発識別符号（42ビット）、着識別符号（28ビット）、ユーザ特定制御チャンネル $USCCH$ （34ビット）、CRC（16ビッ

ト）からなる。図12および図13に示すバーストのうちいずれのフォーマットも16ビットのCRCの検出ビットを備えており、誤り検出が可能である。

【0129】図12に示すフォーマットでは、1バーストあたり情報ビット $I$ の196ビットがCRC検査ビットとCRCを掛けられるビットを加えた値である。図13に示すフォーマットでは、1バーストあたり制御信号 $CAC$ の $62+124=186$ ビットがCRC検査ビットとCRCを掛けられるビットを加えた値である。

【0130】このうち、図12に示すフォーマットでは、1バーストあたり低速付随制御チャンネル $SA$ とトラヒックチャンネル $TCH$ の $16+160=176$ ビットが認証用情報の送受に使用できる。また、図13に示すフォーマットでは、1バーストあたりユーザ特定制御チャンネル $USCCH$ の $62+34=96$ ビットが認証用情報の送受に使用できる。

【0131】このバースト構成に沿ったCRCで誤りを検出する機能を用いた時に、認証用情報を全て送り終えるまでの時間を見積もる。ここでは、通信における呼損率を1%とし、これと同じ程度の確率の失敗は許容するものとする。

【0132】CRC16bitを用いたとき、本当は誤りがあるのに見逃す確率は、 $2^{-16}$ 、おおよそ $1.5 \times 10^{-5}$ でおさえられる。これは上記の1%より十分小さいので、CRCはほぼ完全に誤りを発見できると仮定する。

【0133】このとき、伝送路の平均ビット誤り率を $\epsilon$ とすると、CRC検査ビットとCRCをかけられるビットの計 $n$ ビットが全て誤りなしで伝送できる確率（スループット） $\eta$ は、 $\eta = (1 - \epsilon)^n$ となる。

【0134】ここで、伝送路のビット誤り率の最悪値 $10^{-2}$ を当該伝送路がとるとすると、スループット $\eta$ は、図12のフォーマットを用いた場合では、0.139、図13のフォーマットでは、0.154となる。

【0135】一方、認証方式として、RSA、エルガマルの両方式を候補とすると、署名をして送り返すビット数は、512、1024、2048の3通りが考えられる。これだけのビット数を前述のフォーマットを用いて分割して送る場合に必要バーストの数を $K$ とすると、図12のフォーマットで512ビット送受するには $K=3$ であり、図13のフォーマットで2048ビット送受するには、 $K=22$ である。

【0136】また、認証に費やしてよい時間を $t$ 秒とすると、図12、図13のフォーマットとも1バースト送信するのに5ミリ秒を要するから、 $t$ 秒間に送信できるバーストの数は $N$ は、 $N = t / (5 \times 10^{-3}) = 200t$ である。

【0137】ここで、上記のビット数だけの認証用情報を誤り無く全てを送ることに失敗する確立は、「スループット $\eta$ のパケット通進路で、 $N$ 回パケットを送信したが、 $K$ 回未満しか誤り無く送れない確率 $P$ 」に等しい。

すなわち、

$$P = (1 - \eta)^{N + {}^N C_1 \times \eta \times (1 - \eta)^{N-1} + \dots + {}^N C_{K-1} \times \eta^{K-1} \times (1 - \eta)^{N-K+1}} \quad (1)$$

このPを計算すると、図12のフォーマットで512ビット送受する場合、 $N=30$ でPは約6.9%、 $N=60$ でPは約0.7%となる。したがって99.3%の確率で認証情報の送信を完了するには約0.3秒かかる。図13のフォーマットで2048ビット送受するには、 $N=200$ でPは約2.9%、 $N=225$ でPは約0.05%となり、99.95%の確率で認証情報の送信を完了するには約1.125秒かかる。

【0138】なお、認証を受ける側が上記のような認証情報を送り返す前に、認証をする側が認証を受ける側に送るデータの長さは、せいぜい上記の送り返す情報の長さ以下である。

【0139】(1)の計算からわかるように、確率Pは、送信完了に必要なバーストの数によって大きく左右される。

【0140】したがって、認証に関わる往復の伝送に必要な時間は、図12のフォーマットで512ビット送受する場合では、最小0.3秒、最大0.6秒、図13のフォーマットで2048ビット送受する場合では、最小1.125秒、最大2.25秒となる。また、通常のハードウェアで処理を行うRSA暗号を用いた認証の場合、認証を受ける側が上記のような認証情報を生成するのに必要な計算処理の時間は、0.1~2秒程度である。

【0141】したがって、認証に伴う情報の送受と処理に要する時間は、合計すると0.4~4.25秒程度と\*

$$\{1 - (1 - \eta)^N\}^K$$

この確率を99%以上にするために必要な各バーストの送出回数Nを(2)式から計算すると、図12のフォーマットで512ビット送受する場合、39回となる。したがって99%の確率で認証情報の送信を完了するには

$$(0.005 \text{ 秒} \times 39) \times 3 = 0.585 \text{ 秒}$$

かかる。図13のフォーマットで2048ビット送受するには、46回となり、99%の確率で認証情報の送信を完了するには

$$(0.005 \text{ 秒} \times 46) \times 2 = 0.46 \text{ 秒}$$

かかる。

【0149】また既述の通り、認証を受ける側が上記のような認証情報を送り返す前に、認証をする側が認証を受ける側に送るデータの長さは、せいぜい上記の送り返す情報の長さ以下である。

【0150】(2)の計算からわかるように、認証情報送出に必要な時間は、分割バースト数Kに大きく左右される。

【0151】したがって、認証に関わる往復の伝送に必要な時間は、図12のフォーマットで512ビット送受

\*なる。

【0142】本実施例に拠れば、確実な認証情報の送受が、比較的短い時間で可能となる利点がある。

【0143】なお、ここでは誤り検出符号のみを適用したが、誤り訂正符号を併用し、伝送路のスループットを向上することも考えられる。

【0144】図14に示す実施例では、認証情報を、適当な長さのバーストに分割し、複数回送信するものである。

【0145】ここでは、既述の第2の実施例のバースト構成例を利用して説明する。

【0146】既述の通り、認証方式として、RSA、エルガマルの両方式を候補とすると、署名をして送り返すビット数は、512、1024、2048の3通りが考えられる。これだけのビット数を前述のフォーマットを用いて分割して送る場合に必要なバーストの数をKとすると、図12のフォーマットで512ビット送受するには $K=3$ であり、図13のフォーマットで2048ビット送受するには、 $K=22$ である。

【0147】ここで、必要な各バーストの送出回数をNとする。スループット $\eta$ の packets 通進路で、N回 packets を送信して少なくとも1回誤り無く送ることのできる確率は、 $1 - (1 - \eta)^N$ である。

【0148】このN回の送出を分割数Kだけ繰り返したとき、K個の分割したバーストが全て少なくとも1回誤り無く送ることのできる確率は、

$$(2)$$

する場合では、最小0.6秒、最大1.2秒、図13のフォーマットで2048ビット送受する場合では、最小5.1秒、最大10.2秒となる。

【0152】また、通常のハードウェアで処理を行うRSA暗号を用いた認証の場合、認証を受ける側が上記のような認証情報を生成するのに必要な計算処理の時間は、0.1~2秒程度である。

【0153】したがって、認証に伴う情報の送受と処理に要する時間は、合計すると0.7~12.2秒程度となる。

【0154】この実施例に拠ると、送出回数が固定であるため、あらかじめ処理時間が算出できるという利点がある。これを生かすと、認証情報の処理と他の制御情報の処理とを並列処理する際にスケジューリングを用意に行うことができる。

【0155】また、図11に示す実施例と比較して、比較的認証情報の長さが短い場合に適しているといえる。

【0156】図15に示す実施例では、暗号化情報の復号に伴う誤り検出機能を用いるものである。

【0157】認証にRSA暗号を用いる場合、暗号利用モードのうち、ECB (Electronic Code Book) モードとCBC (Cipher Block Chaining) モードを用いることが考えられる。この二つのモードを利用した場合、伝送路上で1ビット誤った場合、復号側ではブロック全体、あるいはブロック全体および次のブロックにわたって誤りが波及する。

【0158】通常、暗号化する前のデータは、例えばASCIIコード表に従う、あるいは2進化10進数を用いるなど、なんらかのフォーマットに従うようにされる。

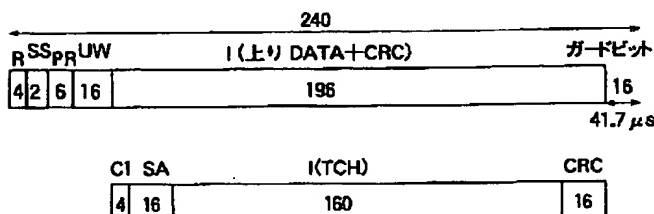
【0159】したがって、ブロック全体に誤りが拡散した復号後のデータは、フォーマットに合わないことで、当該ブロックの伝送の際に誤りが発生したことを検出できる。図15は、ECBモードで、図12に示すフォーマットを用いた場合の例を示す。認証方式としてRSA方式を考える場合、署名をして送り返すビット数は、512、1024の2通りが考えられる。ここでは512ビットを考えると、分割して送る場合に必要なバーストの数Kは3となる。これを連続して送信し、受信側では順次復号し、フォーマットに合うか否かを判断する。ここで、全てのバーストが送られてくるまで待つことなく、フォーマットに合うか否かを判断できる部分から判断をあらかじめ行うことで誤り発生検出を早い段階で行うことも考えられる。誤り発生を検出した場合には、認証を行う側に再送要求を出す。

【0160】また、無線端末PSから基地局CSへの認証用情報の送信には、CRCなどの誤り訂正ビットを設け、基地局CSから無線端末PSへの認証用情報の送信には、誤り訂正ビットを設けず、暗号の復号に伴う誤り検出機能を用いることも考えられる。

【0161】また上述の例とは逆に、基地局CSから無線端末PSへの認証用情報の送信には、CRCなどの誤り訂正ビットを設け、無線端末PSから基地局CSへの認証用情報の送信には、誤り訂正ビットを設けず、暗号の復号に伴う誤り検出機能を用いることも考えられる。

【0162】この実施例に拠ると、CRCなどの誤り検出専用のビットをバーストの中に設ける必要がなくなり、情報速度の向上、あるいは信号の狭帯域化が可能に\*40

【図12】



\* なる。暗号専用の処理装置や高速の演算装置を用いると、認証処理と誤り検出が同時に非常に短時間で行うことができる。

## 【0163】

【発明の効果】以上述べたように本発明によれば、無線通信システムにおける無線端末の正当性確認と鍵共有を同時に、通信量少なく実現できる。また、無線端末と基地局相互の正当性確認と鍵共有を実現する場合にも、従来方式よりも通信量が少なくなる。

## 【図面の簡単な説明】

【図1】 無線端末の認証方式および無線端末と基地局の鍵共有方式の基本構成を表す図

【図2】 無線通信システムの構成図

【図3】 第1の実施例である無線端末の認証・鍵共有手順を示す図

【図4】 第2の実施例である無線端末の認証・鍵共有手順を示す図

【図5】 第2の実施例中の鍵共有関数の構成を示す図

【図6】 無線端末と基地局の相互認証方式と鍵共有方式の基本構成を表す図

【図7】 第3の実施例である無線端末と基地局の相互認証・鍵共有手順を示す図

【図8】 第4の実施例である無線端末と基地局の相互認証・鍵共有手順を示す図

【図9】 認証のシーケンスを示す図。

【図10】 片方向のみの送受信を用いた認証のシーケンスを示す図。

【図11】 認証用情報をバーストに分割し、自動再送手順を用いた場合の説明図。

【図12】 バーストのフォーマット図

【図13】 バーストのフォーマット図

【図14】 認証用情報をバーストに分割し、複数回送信する場合の説明図。

【図15】 暗号化情報の復号に誤り検出機能を用いる場合の説明図。

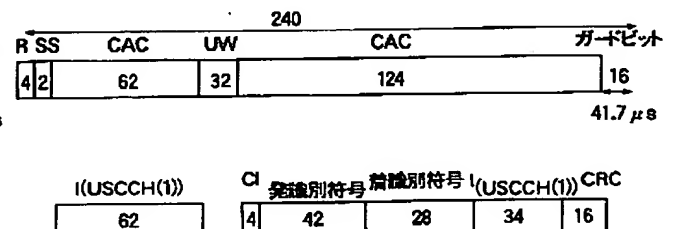
## 【符号の説明】

CC……制御局

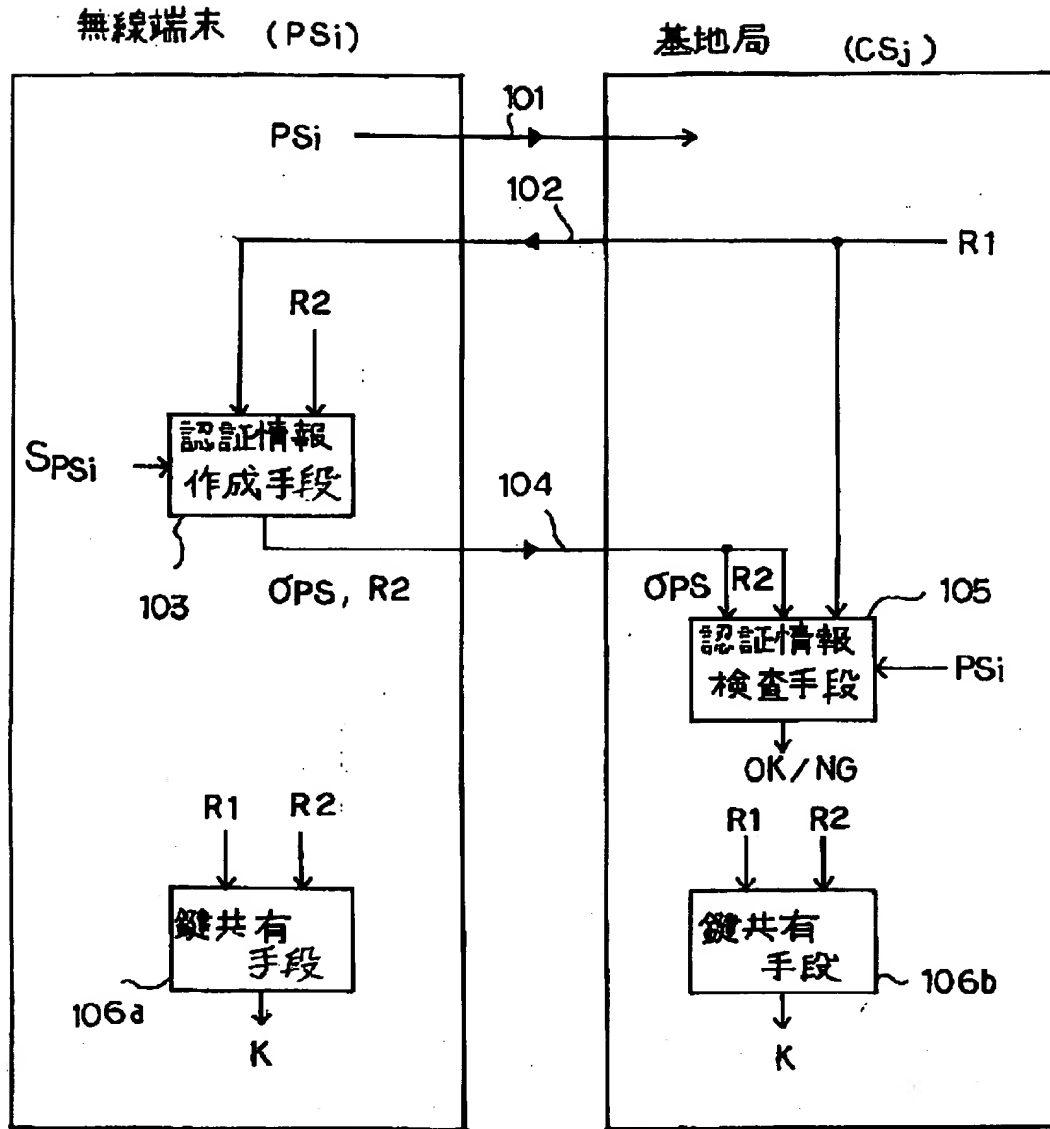
CS……基地局

PS……無線端末

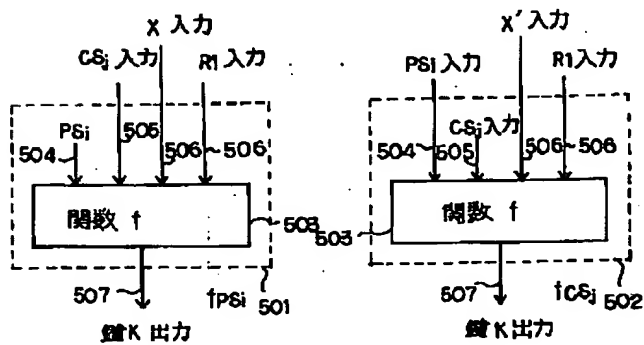
【図13】



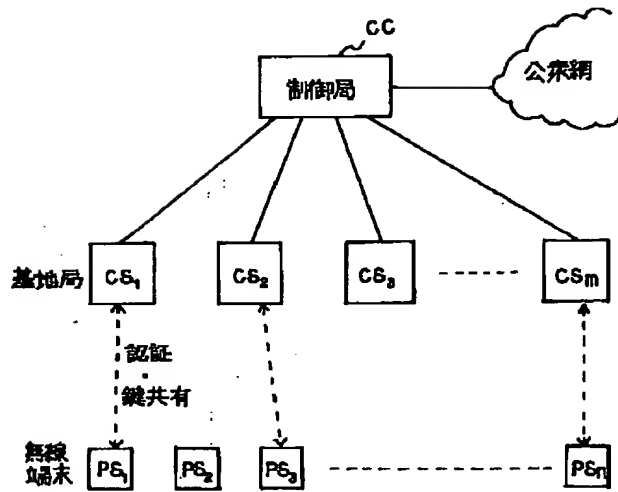
【図1】



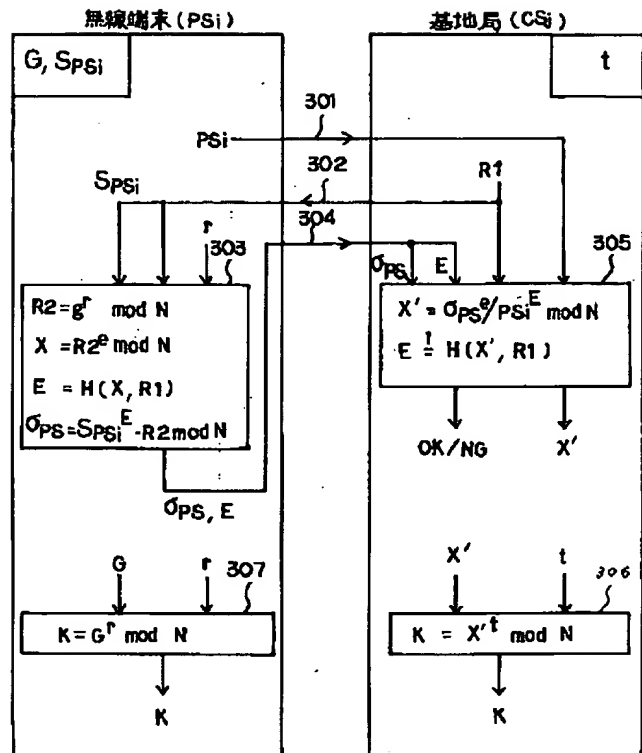
【図5】



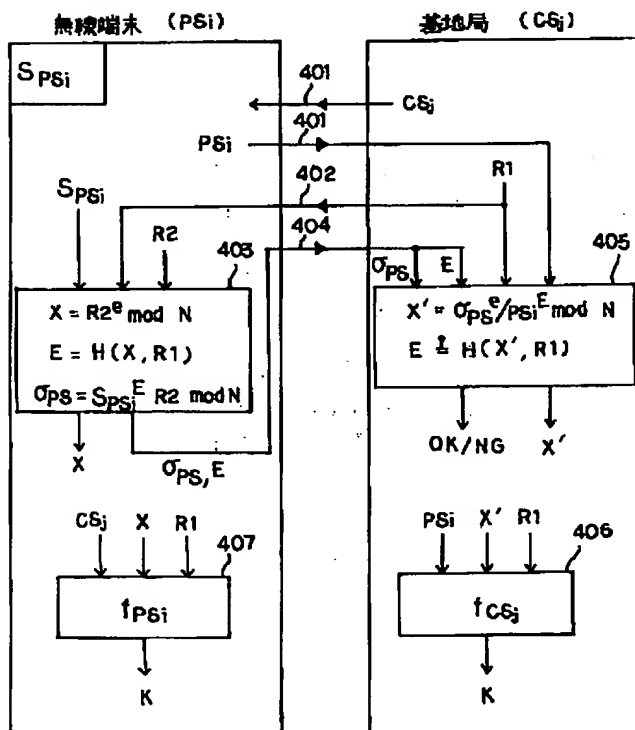
【図2】



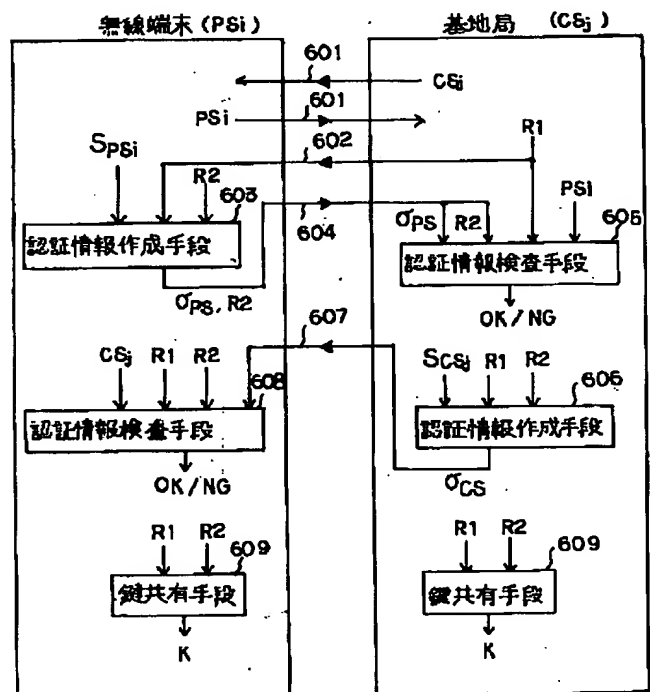
【図3】



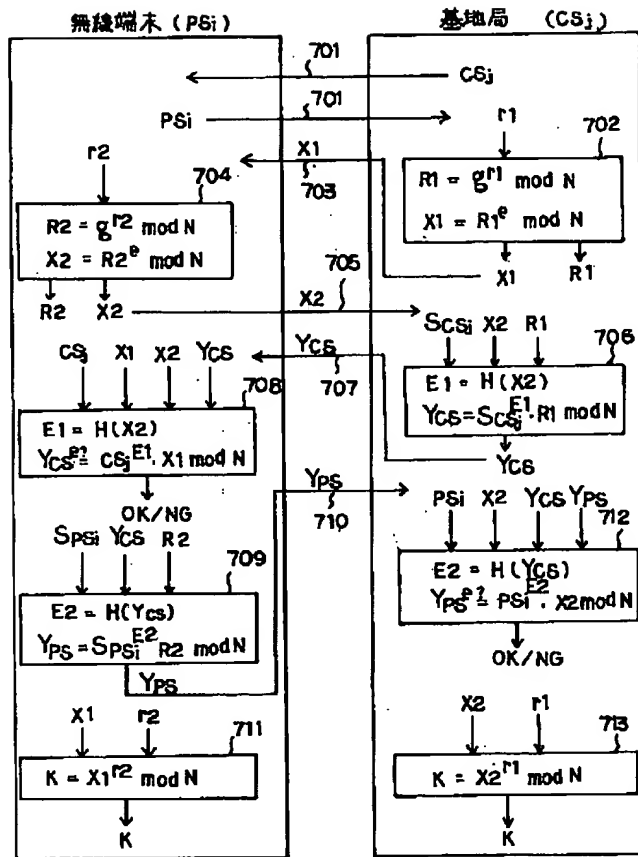
【図4】



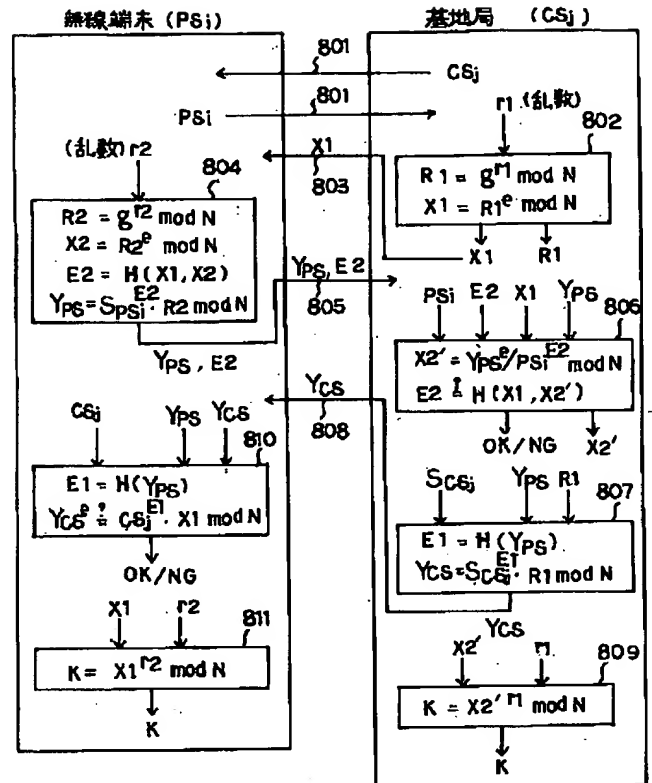
【図6】



【図7】

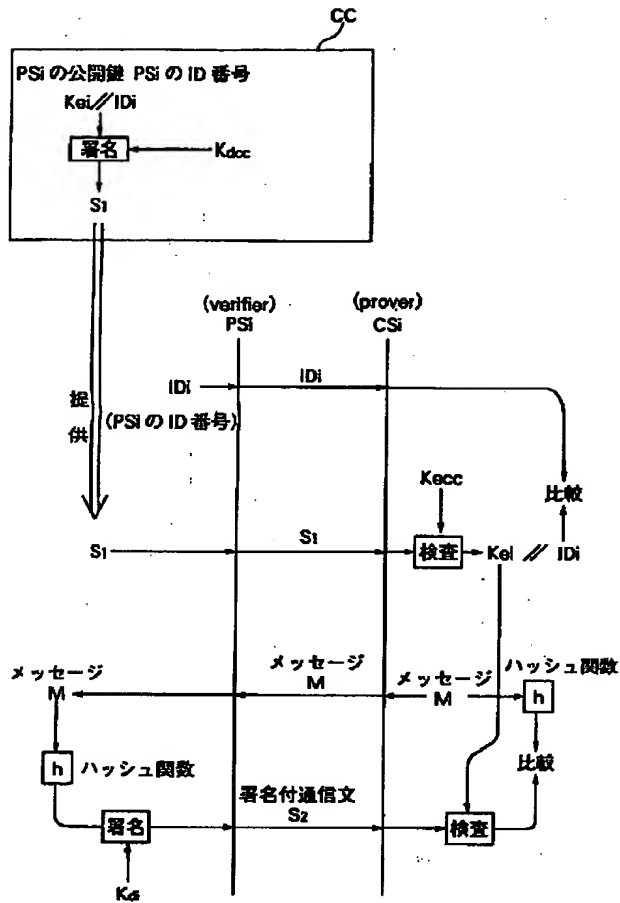


【図8】

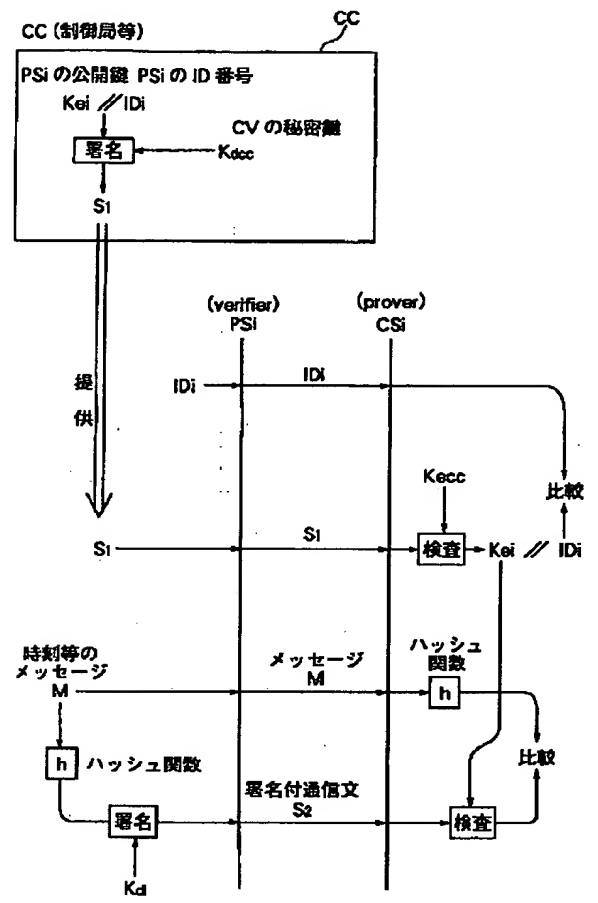




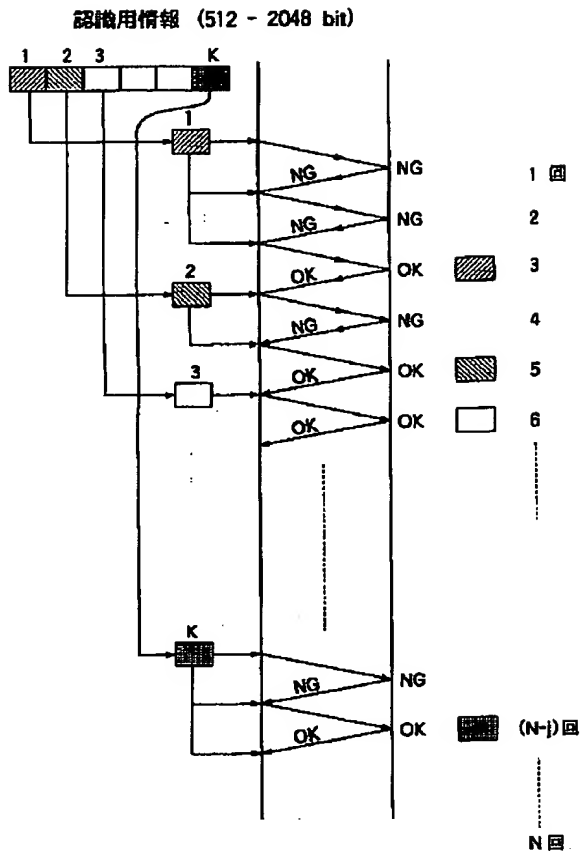
【図9】



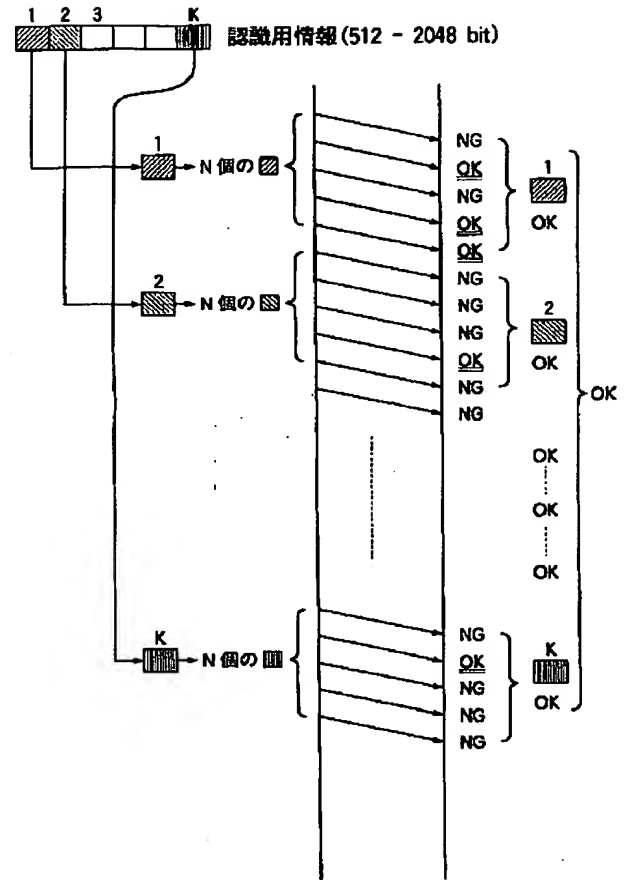
【図10】



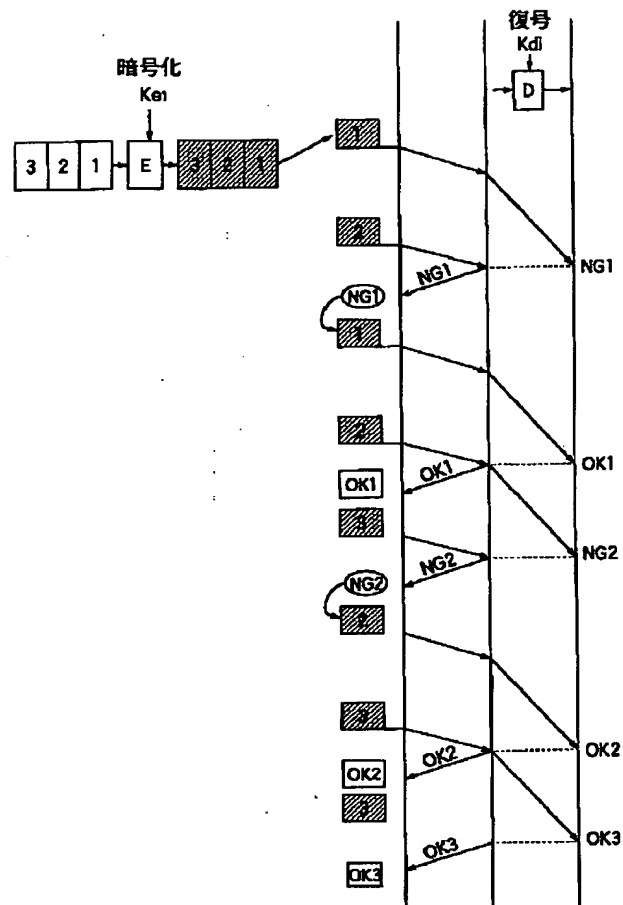
【図 1 1】



【図 1 4】



【図15】



フロントページの続き

(72)発明者 小倉 浩嗣  
 神奈川県川崎市幸区小向東芝町1番地 株  
 式会社東芝総合研究所内